UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/023,852 | 12/21/2001 | Paul Nicholas Gartside | 01.122.01 | 5732 |

7590 08/15/2007

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

| EXAMINER | |
|---|---|
| BESROUR, SAOUSSEN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 08/15/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/023,852 | GARTSIDE ET AL. | |
| | Examiner | Art Unit | |
| | Saoussen Besrour | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38 and 40-47, 49-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8-17,19-22,24-33,35-38,40-47,49 and 50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/13/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to amendment filed 5/31/2007. Claims 1, 9, 41, were amended. Claims 2, 7, 18, 23, 34, 39 and 48 were cancelled. New claims 49 and 48 were added. Claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38 and 40-47, 49-50 are pending.

Applicant's arguments/ amendments with respect to the claims have been fully considered but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

### *Claim Rejections - 35 USC § 101*

2. Corrections to the claims were received 5/31/2007. Thus previous 101 rejection has been withdrawn.

### *Response to Arguments*

Applicant's arguments filed 5/31/2007 have been fully considered but they are not persuasive.

3. Regarding Applicant's argument on page 14 of arguments that Nambu does not teach "identifying one or more class of malware threat against which said mobile computing device us to be protected", Examiner respectfully disagrees and would like to point out 0071 where it states that the pattern files can be referred to as signature files or virus definition files, where it is a code of particular virus, interpreted by examiner as the class of malware. Furthermore, 0075 –0078 states that the maintenance server

stores information on all the related user terminals based on the user-related information, it provides the terminals with updated vaccine and pattern files. 0083 discloses protecting against the new virus, which the device is to be protected against. 0089 states that the information 54a and 54b, include information of the user's device, such as applied pattern name for that user device. 0095 states that the new anti-virus program reads user information and acquires the software related information from each use, including pattern file.

4. Regarding Applicant's argument on page 15 of arguments that Nambu does not teach "generating from said master malware...against which said mobile computing device is to be protected", Examiner respectfully disagrees and would like to point out 0093, 0095-0096, which states software designated information from each user.

5. Regarding Applicant's argument on page 16 of arguments that Nambu does not teach "transferring computer files an corresponding threat data ...to which each of said mobile computing device is vulnerable", Examiner respectfully disagrees and would like to point 0083 where it states transferring vaccine software and pattern file.

6. Regarding Applicant's argument on page 18 of arguments that Nambu does not teach "wherein said one or more classes of malware...and classes for which it is desired to protect said mobile computing device according to user defined policies", Examiner respectfully disagrees and would like to point out, 0089 and 0100-0103, where it states determining that the vaccine software and data pattern file have not been updated for new virus, then based on the determination obtaining up to date vaccine from user information.

7. Regarding applicant's argument on page 20, that Nambu does not teach "wherein user controlled policy datat is used in combination with said threat data to control against ..." Examiner respectfully disagrees and would like to point out, 0089 and 0100-0103, where it states determining that the vaccine software and data pattern file have not been updated for new virus, then based on the determination obtaining up to date vaccine from user information.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1, 3-6, 8-16, 17, 19-22, 24-32, 33, 35-38 and 40-47 and 49-50** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nambu (US 2002/0124182) in view of Hershberg et al. (US 2003/0022657).

As per **claim 1**, Nambu discloses: obtaining code operable to obtain from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality of classes of malware threat (0071-0072); identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected (0072-0074)(it is known within existing malware definition data to include information that classifies the malware items using classes); generating code operable to generate from said master malware

definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identifies within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected (0075, 0077, 0078); wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data (0080-0083); wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed locatrion computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable (0074, 0075, 0077); wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for [tailoring] said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing device is vulnerable (0078, 0081, 0108 by checking the present condition of the usert device, user info processing program 51 which determines condition of the user terminal); wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies (0078, 0081, 0108 acquiring vaccine via user

information processing program which determined condition of the user terminal). Nambu does not explicitly teach tailoring the downloads from the server for a specific device. However, Hershberg et al. discloses tailoring downloads for specific devices depending on whether the device needs the program or not (0089, 0094). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Hershberg in conjunction with the teachings of Nambu for the benefit of accommodating downloads from the server to clients with low bandwidth and low processing space (wireless devices), thereby greatly reducing the request to display delay.

As per **claim 17**, Nambu discloses: obtaining code operable to obtain from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality of classes of malware threat (0071-0072); identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected (0072-0074) (it is known within existing malware definition data to include information that classifies the malware items using classes); generating code operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identifies within

said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected (0075, 0077, 0078); wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data (0080-0083); wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed locatrion computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable (0074, 0075, 0077); wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for [tailoring] said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing device is vulnerable (0078, 0081, 0108 by checking the present condition of the usert device, user info processing program 51 which determines condition of the user terminal); wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies (0078, 0081, 0108 acquiring vaccine via user information processing program which determined condition of the user terminal). Nambu does not explicitly teach tailoring the downloads from the server for a specific

device. However, Hershberg et al. discloses tailoring downloads for specific devices depending on whether the device needs the program or not (0089, 0094). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Hershberg in conjunction with the teachings of Nambu for the benefit of accommodating downloads from the server to clients with low bandwidth and low processing space (wireless devices), thereby greatly reducing the request to display delay.

As per **claim 33**, Nambu discloses: obtaining code operable to obtain from a data source master malware definition data, said malware definition identifying a plurality of malware each belonging to one of a plurality of classes of malware threat (0071-0072); identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected (0072-0074) (it is known within existing malware definition data to include information that classifies the malware items using classes); generating code operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identifies within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected (0075, 0077, 0078); wherein said obtaining code, said identifying code and said generating code are executed by a fixed

location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data (0080-0083); wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed locatrion computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable (0074, 0075, 0077); wherein only a subset of master malware definition data is used to generate said mobile computing device malware definition data for [tailoring] said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing device is vulnerable (0078, 0081, 0108 by checking the present condition of the usert device, user info processing program 51 which determines condition of the user terminal); wherein said one or more classes of malware threat against said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies (0078, 0081, 0108 acquiring vaccine via user information processing program which determined condition of the user terminal). Nambu does not explicitly teach tailoring the downloads from the server for a specific device. However, Hershberg et al. discloses tailoring downloads for specific devices depending on whether the device needs the program or not (0089, 0094). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention

was made to use the teachings of Hershberg in conjunction with the teachings of Nambu for the benefit of accommodating downloads from the server to clients with low bandwidth and low processing space (wireless devices), thereby greatly reducing the request to display delay.

As per **claims 3, 19 and 35**, rejected as applied to claims 1, 17 and 33. Furthermore Nambu discloses: said fixed location computing device is a user computer having communication link with said mobile computing device (0074).

As per **claims 4, 20 and 36**, Rejected as applied to claims 1, 17 and 33. Furthermore nambu discloses: when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer filed respectively stored by said mobile computing device and said fixed location computing device are synchronized (0074, 0075, 0077 various user terminals).

As per **claims 5, 21 and 37**, rejected as applied to claims 4, 20 and 36. Furthermore, Nambu et al. discloses: said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronization (0075, 0077).

As per **claims 6, 22 and 38**, rejected as applied to claims 4, 20 and 36. Furthermore, Nambu discloses: when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware

definition data stored on said mobile computing device and said fixed location computing device are compared, and if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device (0078-0079).

As per **claim 8, 24 and 40**, rejected as applied to claims 1, 17 and 33. Furthermore, Nambu et al. discloses: wherein user controlled policy data us used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data (0082).

As per **claims 9, 25 and 41**, rejected as applied to claims 1, 17 and 33. Furthermore, Nambu discloses: different types of operating system computer program used by mobile computing device (0074, various devices).

As per **claim 10, 26 and 42**, rejected as applied to claims 1, 17 and 33. Furthermore, Nambu et al. discloses: said fixed location computer device detects to which mobile computing devices it transfer computer files by detecting installation upon fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices (0078).

As per **claim 11, 27 and 43**, rejected as applied to claims 1, 17 and 33. Furthermore, Nambu discloses: fixed location computing device also transfers a

malware scanner computer program from said data source to said mobile device (0078).

As per **claim 12**, rejected as applied claims 1, 17 and 33. Furthermore, Nambu discloses said fixed location computing device checks for updated master malware definition data becoming available from said data source, if such updated master malware definition become available, then repeats steps of obtaining, identifying and generating (0070, 0083).

As per **claim 13, 29 and 45**, rejected as applied to claim 11, 27 and 43. Furthermore, Nambu discloses: said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an update malware scanner computer program becomes available, then obtains said updated malware scanner computer program for transfer to said mobile computing device (0070, 0083).

As per **claim 14, 30 and 46**, rejected as applied to claim 1, 17, 33. Furthermore, Nambu et al, discloses: said master malware definition is data also used to protect said fixed location computing device from malware (0112).

As per **claim 15 and 31**, rejected as applied to claims 1 and 17. Furthermore, Nambu discloses: said fixed location computing device is connected to said data source by a fixed interner link (Fig. 5).

As per **claims 16 and 32**, rejected as applied to claims 1 and 17. Furthermore, Iathi et al discloses: said item of malware include one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image (0078).

As per **claim 47**, rejected as applied to claim 1. Furthermore, Nambu discloses: said fixed location device stores policy data including user defined settings identifying the manner in which said profile data is to be intercepted (0074, 0075, 0082).

As per **claim 49**, rejected as applied to claim 1. Furthermore, Nambu discloses wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to said classes of malware threat known to pose a problem to an operating system of said mobile computing device (0100-0103).

As per **claim 50**, rejected as applied to claim 1. Furthermore, Nambu discloses wherein at least a portion of said mobile computing device malware definition data poses a problem only to said mobile computing device and not to said fixed location computing device (0100-0103).

***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saoussen Besrour whose telephone number is 571-272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SB
August 9, 2007

CHRISTOPHER REVAK
PRIMARY EXAMINER